Хорошко Володимир Олексійович, доктор технічних наук, професор, професор кафедри безпеки інформаційних технологій Національного авіаційного університету.
Volodymyr Khoroshko, doctor of technical sciences, professor, professor of the department of security of information technologies of the National Aviation University.
E-mail: professor_va@ukr.net.
Orcid ID: 0000-0001-6213-7086.

Браіловський Микола Миколайович, кандидат технічних наук, доцент, доцент кафедри кібербезпеки і захисту інформації Київського національного університету імені Тараса Шевченка.
Mykola Brailovskyi, PhD in Engineering Science, Associate Professor, Associate Professor of department of Cybersecurity and Information Protection of the Taras Shevchenko National University of Kyiv.
E-mail: bk1972@ukr.net.
Orcid ID: 0000-0002-3148-1148.

Хохлачова Юлія Євгеніївна, кандидат технічних наук, доцент, доцент кафедри безпеки інформаційних технологій Національного авіаційного університету.
Yuliia Khokhlachova, PhD of technical sciences, associate professor, associate professor of the department of security of information technologies of the National Aviation University.
E-mail: yuliiahohlachova@gmail.com.
Orcid ID: 0000-0002-1883-8704.

Капустян Марія Вікторівна, кандидат технічних наук, доцент, доцент кафедри систем і захисту інформації Хмельницького національного університету.
Mariia Kapustian, PhD of technical sciences, associate professor, associate professor of the department of systems and information protection of Khmelnitsky National University.
E-mail: kapustian.mariia@gmail.com.
Orcid ID: 0000-0001-9200-1622.

DOI: 10.18372/2410-7840.24.17266
УДК 004.681.3

МАТРИЧНИЙ ПОМНОЖУВАЧ ЗА МОДУЛЕМ ДЛЯ КРИПТОГРАФІЧНИХ ПЕРЕТВОРЕНЬ

Максим Луцький, Сахибай Тинимбаєв, Сергій Гнатюк, Рат Бердібаєв, Юлія Поліщук

Сьогодні для шифрування даних найбільш широко застосовують три види шифраторів: апаратні, програмно-апаратні і програмні. Їх основна відмінність полягає не лише у способі реалізації шифрування та ступеня надійності захисту даних, але й ціною, що часто стає для користувачів визначальним чинником. Незважаючи на те, що ціна апаратних шифраторів істотно вища ніж програмних, різниця в ціні не спів-ставна із значним підвищенням якості захисту інформації. Апаратне шифрування має низку вагомих переваг перед програмним шифруванням, одна з яких – більш висока швидкодія. Апаратна реалізація гарантує цілісність процесу шифрування. При цьому генерування і збереження ключів, а також шифрування, здійснюється у самій платі шифратора, а не в операційній пам'яті комп'ютера. З огляду на це, розробка швидкодіючих операційних блоків апаратних процесорів для асиметричного шифрування, не дивлячись на їх високу вартість, є актуальною науковою та прикладною задачею. У цій статті проводиться аналіз сучасних підходів до множення чисел за модулем, виділено їх сильні та слабкі сторони. Досліджено алгоритм множення з покроковим формуванням часткових і проміжних залишків, що в свою чергу, не потребує ви-конання попередніх обчислень, а всі обчислення не виходять за діапазон розрядної сітки модуля. Як результат, розроблено синхронний матричний помножувач, який містить n блоків схем I, n-1 FPR і єдиний FIR з регістром проміжного залишку, що буде корисним для криптографічних перетворень в системах з підвищеними вимогами до швидкодії та рівня інформаційної безпеки (наприклад, в критичній інформаційній інфраструктурі).

Ключові слова: *криптосистема з відкритим ключем, апаратне шифрування, формувач залишків, помножувач.*

ВСТУП

В асиметричних криптосистемах процедура шифрування і дешифрування даних проводиться піднесенням числа a до степеню x за модулем P (a^x modP), якого можна реалізувати програним, програмно-апаратним і апаратним засобами [1, 2].

Апаратне шифрування має низку вагомих переваг перед програмним шифруванням, одна з яких (і ймовірно найбільш суттєва) – більш висока швидкодія. Апаратна реалізація гарантує цілісність процесу шифрування. При цьому генерування і збереження ключів, а також шифрування здійснюється безпосередньо у самій платі шифратора, а не в операційній пам'яті комп'ютера.

Сьогодні, розробка швидкодіючих операційних блоків апаратних процесорів для асиметричного шифрування, не дивлячись на їх високу вартість, є актуальною науково-прикладною задачею.

З огляду на зазначене, основною метою статті є розробка матричного помножувача за модулем для криптографічних перетворень.

Аналіз підходів до множення за модулем

Множення чисел за модулем можна виконувати 2 способами. У першому випадку операція розбивається на два етапи. На першому етапі n-розрядні числа A і B перемножуються і формують 2n-розрядне число C. На другому етапі добуток C = A*B приводиться за модулем P.

На сьогодні накопичено великий досвід в розробці швидкодіючих цілочисельних помножувачів і засобів для зведення в квадрат. До них відносяться: помножувач Брауна, Уоллеса, помножувачі Дадда, систолічні та ведичні помножувачі і квадратори, де складність обчислення складає O(n^2) бітових операцій. Але ці помножувачі дуже ефективні при обчислені «мало-розрядних» чисел, які найшли широке використання при побудові операційних блоків комп'ютерів різного класу [3].

У криптографії для множення багаторозрядних чисел, що дозволяє обчислити необхідний добуток швидше, ніж за O(n^2) кроків (бітових операції), знайшли широке застосування метод Карацуба [4], складність якого дорівнює O(n^lo _2 3), алгоритм Тоом-Кука [5] зі складністю порядку O(⟦n2⟧ ^√(⟦2log⟧ _2 n)) бітових операцій. Алгоритм Шенгахе-Штрассен [6] дозволяє помножити два n-розрядних числа за O (nlogn logn) бітових операцій. Операція приведення за модулем, яка виконується на другому етапі, є отримання залишку від ділення C = A * B на модуль P. У роботі [7] проаналізовані різні способи приведення чисел за модулем. Показано, що найефективнішим засобом побудови є пристрій приведення за модулем на основі ділильного пристрою. До складу такого пристрою входить формувач часткових залишків. На основі формувачів часткових залишків легко реалізуються високопродуктивні матричні і конвеєрні пристрої приведення чисел за модулем [8-12].

У другому способі множення за модулем за допомогою використання алгоритму ділення великих чисел. Наприклад, для алгоритму Баррета [13] потрібні попередні обчислення константи μ=⌊d^2m/N⌋, де d=2^k, k- розмір слова в бітах, m-кількість слів в модулі N.

Ефективність алгоритму Баррета повністю залежить від того, наскільки ефективно будуть виконані попередні обчислення, які виконуються розподілом великих чисел.

Для алгоритму Монтомері потрібно попереднє вирахування константи ⟦"r⟧ ^2 (modN)", використовуючи ділення з залишком [14, 15].

У третьому способі процес множення чисел за модулем виконується за велику кількість кроків, де його кількість визначається розрядністю множника.

У статті розглядається множення чисел за модулем, де множення починається з аналізу молодших розрядів. У такому помножувачі на кожному кроці множення виконуються наступні дії:

1) формувачем часткового залишку FPRi обчислюється частковий залишок ri, для чого попередній частковий залишок ri-1, зрушений на один розряд в бік старшого розряду приводиться до модулю P, тобто ri=2ri-1modP. При формуванні першого часткового залишку ri в якості попереднього часткового залишку приймається A, тобто ri=A1;

2) частковий залишок ri логічно множиться на i-біт множника B блоком логічної схеми Ii;

3) обчислюється проміжний залишок Ri шляхом складання часткового залишку ri з попереднім проміжним залишком Ri-1 за модулем P, тобто Ri=(ri+ Ri-1)modP.

Після виконання n кроків множення формується результат R-Rn-1=(rn-1+Rn-2)modP.

У роботі [16] наведений алгоритм множення чисел за модулем реалізований згідно асинхронної матричної системи, яка складається з n блоків схем I, n-1 FPR і n-1 FIR (формувач проміжних залишків). Недоліком цієї схеми є складність в апаратній реалізації. Для усунення зазначеного недоліку у цій статті пропонується розроблений авторами синхронний матричний помножувач, який містить n блоків схем I, n-1 FPR і єдиний FIR з регістром проміжного залишку. Робота помножувача синхронізується за допомогою розподільника рівнів.

ОСНОВНА ЧАСТИНА

Функціональна схема синхронного помножувача за модулем з матричною структурою наведена на Рис. 1. До складу помножувача входять n-розрядний регістр множника RgB, регістр множеного RgA і регістр модуля RgP, блок синхронізації Бл. СИНХ, що генерує сигнали-рівні для блоку схем I0÷In-1. На входи Бл. СИНХ подається сигнал ПУСК, тактові сигнали Clock, двійковий код сигналу числа розрядів множника – n. За сигналом ПУСК виробляється сигнал ПРИЙОМ, за яким розряди множника B приймаються в регістр RgP через блоку схем 3'.

До складу Бл. СИНХ входять двійковий лічильник і дешифратор. Стан лічильника дешифрується і на їх виходах виробляються рівні сигналів для I0÷In-1.

Сигналом ПУСК також двійковий код числа n записується в двійковий лічильник і дає дозвіл для проходження тактового сигналу Clock на вхід лічильника. До складу помножувача також входять формувачі часткових залишків FPR.1÷FPR.n-1 і схеми I0÷In-1, схема АБО1 і формувач проміжних залишків FIR з регістром проміжного залишку. Вивід результату множення I4' після надходження синхросигналу un-1 від Бл. СИНХ через елемент затримки ЄЗ.

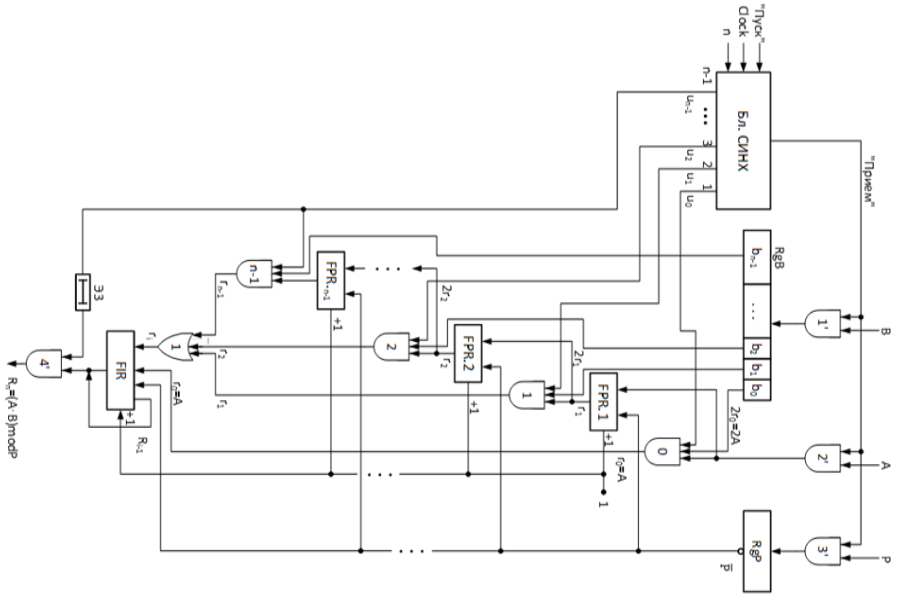

Рис. 1. Функціональна схема матричного помножувача за модулем

Значення модуля P з інверсного виходу RgP подається на входи всіх FPR.1÷FPR.n-1 и FIR. За сигналом ПРИЙОМ множник A через блок схем I2' подається на входи блоку схем I0 із зсувом на один розряд в бік старшого розряду подається на вхід FPR.1. На інші входи блоку I0 подається значення молодшого розряду регістра RgB – b0 і керуючий рівень u0 з виходу Бл. СИНХ.

Вихід I0 пов'язаний з регістром FIR. Вихід FPR.1 пов'язаний зі входом блоку схем I1. Інші входи I1 пов'язані з виходами регістра RgB і Бл. СИНХ, за якими надходять значення біта b1 і керуючий рівень u1. Вихід блоку I1 пов'язаний зі входом схеми АБО1.

Значення коду з виходу FPR.1 із зсувом на один розряд в бік молодшого розряду подається на вхід FPR.2. У свою чергу, вихід FPR.2. пов'язаний із входами блоку схем I2, на інші входи яких подається значення розряду b2 з регістра RgB і керуючий рівень u2 з Бл. СИНХ.

Вихід блоку схем I2 пов'язаний зі входом схеми АБО1. Аналогічні зв'язку є між FPR.3÷FPR.n-2 і блоками схем I3÷Иn-2. На входи FPR.n-1 подається значення коду з виходу FPR.n-2 із зсувом на один розряд в бік молодшого розряду і код модуля P з виходів RgP. Вихід FPR.n-1 пов'язаний зі входом блоку схем In-1, куди надходять також значення старшого розряду bn-1 регістра RgB і керуючий сигнал un-1 з Бл. СИНХ. А вихід блоку схем In-1 пов'язаний зі входом АБО1. На рис. 2 наведена структура FPR, який слугує для формування часткового залишку ri від подвоєного попереднього залишку за модулем P: ri=2ri-1 modP.

FPR складається з двійкового суматора Add і мультиплексора MS, що містить блоки схем I1 і I2 і схеми АБО1.

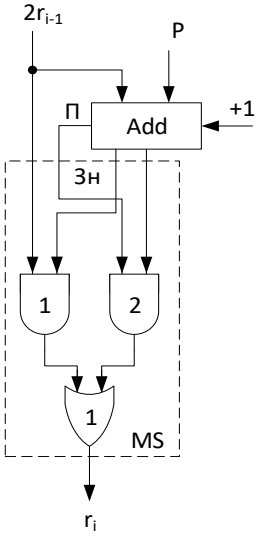

Рис. 2. Структура FPR

На входи суматора подається подвоєний частковий залишок 2_{ri-1}, зворотний код модуля $\overline{P}$ і одиничний сигнал +1. У результаті виконання операції $r_i=2_{ri-1}\ mod\overline{P}+1$ на виході суматора формується різниця зі своїм знаком ЗН. Якщо при цьому ЗН = 1, то на виходи FRP передається код 2_{ri-1} ($2_{ri-1}<P$). При цьому, перенесення зі знакового розряду П = 0. Якщо ЗН = 0, то на виходи FPR передається результат віднімання $2_{ri-1}-P$ ($2_{ri-1}\geq P$).

На рис.3 наведено структуру формувача проміжних залишків FIR, до складу якого входять суматор Add, FPR, схеми $АБО_2$ і регістр проміжних залишків RgR. Вихід регістра RgR пов'язаний зі входом Add, куди передається значення R_{i-1}. Із Рис. 3 неважко помітити, що схема виконує операцію $R_i=(r_i+R_{i-1})modP$.

Розглянемо роботу матричного помножувача чисел за модулем. Після прийому операндів A, B, P у відповідні регістри і двійкового коду числа розрядів множника в Бл. СИНХ надходить перший тактовий імпульс Clock 1 і в двійковий лічильник записується код 1. При цьому на виході 1 Бл. СИНХ виробляється високий рівень u_0, який подається на вхід блоку схем I_0. На інші входи I_0 подається молодший розряд множника b_0 і розряди множника A. При $b_0=1$ на виході блоку схеми I_0 формується частковий залишок $r_0=R_0$, який записується в RgR FIR. Після цього в Бл. СИНХ надходить тактовий сигнал Clock 2 і на виході Бл. СИНХ формується керуючий рівень u_2, який подається на вхід I_2. На інші входи I_2 подаються значення біта b_2 регістра RgB і значення r_2 з виходу $FPR_{.2}$. Виходи блоку схем I_2 подаються на вхід схеми $АБО_1$.

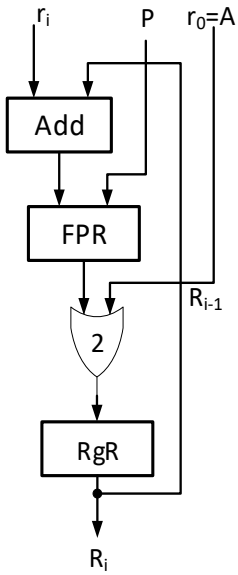

Рис. 3. Структура FIR

Аналогічно формуються часткові залишки $r_3 \div r_n$, які також через схеми $АБО_1$ подаються на вхід FIR. FIR, отримавши часткові залишків, r_i формує R_i за формулою $R_i=(r_i+R_{i-1})modP$.

У табл. 1 наведено приклад виконання операції множення за модулем у синхронному матричному помножувачі, де $A=27_{10}$; $B=23_{10}=10111_2$; $P=35_{10}$. Для зручності, всі арифметичні операції виконані в десятковій системі числення.

Перевірка:

$R=(27x23)mod35=621mod35=26_{10}$

Таблиця 1

Порядок множення чисел за модулем

u_0	u_1	u_2	u_3	u_4
$r_0=A*b_0=27_{10}$	$r_1=2r_0modP=54-35=19_{10}$	$r_2=2r_1modP=38-35=3_{10}$	$r_3=2r_2modP=6mod35=6_{10}$	$r_4=2r_3modP=12mod35=12_{10}$
RgR: = $r_0=A=R_0=27_{10}$	RgR: = $(r_1b_1+R_0)modP=(19+27)mod35=11_{10}$ $R_1=11_{10}$	RgR: = $(r_2b_2+R_1)modP=(3+11)mod35=14_{10}$ $R_2=14_{10}$	RgR: = $(r_3b_3+R_2)modP=(6*0+14)mod35=14_{10}$ $R3=14_{10}$	RgR: = $(r_4b_4+R_3)modP=(12+14)mod35=26_{10}$ $R4=26_{10}$

ВИСНОВКИ

У цій статті проведено аналіз сучасних підходів до множення чисел за модулем, виділено їх сильні та слабкі сторони. Досліджено алгоритм множення з покроковим формуванням часткових і проміжних залишків, що в свою чергу, не потребує виконання попередніх обчислень, а всі обчислення не виходять за діапазон розрядної сітки модуля. Як результат, розроблено синхронний матричний помножувач, який містить n блоків схем I, n-1 FPR і єдиний FIR з регістром проміжного залишку. Отримані результати будуть корисними для криптографічних перетворень в системах з підвищеними вимогами [17] до швидко-дії та рівня інформаційної безпеки (наприклад, в критичній інформаційній інфраструктурі).

ЛІТЕРАТУРА

[1] Tynymbayev S., Ibraimov M., Namazbayev T., Gnatyuk S. Development of pipelined polynomial multiplier modulo irreducible polynomials for cryptosystems, Eastern-European Journal of Enterprise Technologies, 2022, Vol. 1, Issue 4-115, pp. 37-43.

[2] Айтхожаева Е. Ж., Тынымбаев С. Т. Аспекты аппаратного приведения по модулю в ассиметричной криптографии, Вестник НАН РК, №5, Ал-маты 2014, С. 88-93.

[3] Gnatyuk S., Iavich M., Kinzeryavyy V., Okhrimenko T., Burmak Y., Goncharenko I. Improved secure stream cipher for cloud computing, CEUR Workshop Proceedings, 2020, Vol. 2732, pp. 183-197,

[4] Карацуба А. А., Офман Ю. П. Умножение многоразрядных чисел на автоматах. ДАН СССР. 1962, Т. 145, С. 293-314.

[5] Cook S. A., Aanderaa S. O. On the minimum computation time of functions, Trans. AMS, 142 (1969), pp. 291-314.

[6] Шенхаге А., Штрассен В. Быстрое умножение больших чисел. Кибернетический сборник. 1973. вып. 2. С. 87-98.

[7] Ковтун М., Ковтун В. Обзор и классификация алгоритмов деления и приведения по модулю больших целых чисел для криптографических приложений [Электронный ресурс] http:// docplayer.ru/ 30670408-Obzor-i-klassifikaciya-algoritmov-deleniya-i-privedeniya-po-modulyu-bolshih-celyh-chisel-dlya-kriptograficheskih-prilozheniy.html

[8] Патент 2029435: МПК H03M7/18, Петренко В.И., Чипига А.Ф. Комбинационный рекуррентный формирователь остатков: № 5032302 / 24; 20.02. 1995, 3 с.

[9] Патент 2368942: МПК H03M7/18, Петренко В. Н., Сидорчук А. В., Кузьминов Ю. В. Устройство для формирования остатков по произвольному модулю: №02101066858/08; 27.09.2009, Бюл. № 21, 8 с.

[10] Tynymbayev S.T., Aitkhozhayeva Y.Zh., Adilbekkyzy S. High speed device for modular reduction, Bulletin of National academy of sciences of the Republic of Kazakhstan. 2018. Vol. 6, N 376. P. 147-152.

[11] Патент РК №30983, Тынымбаев С.Т., Айтхожаева Е.Ж. Формирователь остатка по произвольному модулю, 19.02.2016, Бюл. №3

[12] Тынымбаев С.Т., Бердибаев Р.Ш., Омар Т., Шайкулова А.А., Магауин Б. Быстродействующие устройства приведения числа по модулю, Матер. IV Междунар. Азиатской школы-семинара «Проблемы оптимизации сложных систем», Кыргызская Республика, оз. Иссыккуль, пансионат «Отель Евразия». - Ч2, 20-31 июля 2018, С. 273-279.

[13] Barrett, P. (1987). Implementing the Rivest Shamir and Adleman Public Key Encryption Algorithm on a Standard Digital Signal Processor. In: Odlyzko, A.M. (eds) Advances in Cryptology — CRYPTO' 86. CRYPTO 1986. Lecture Notes in Computer Science, vol 263. Springer, Berlin, Heidelberg. https:// doi. org/10.1007/3-540-47721-7_24

[14] Montgomery P.L. Modular Multiplication without Trial Division, Math. Compulation. Vol. 44, N 170 (Apr., 1985), P. 519-521. DOI: 10.20307/2007970.

[15] Pisek Eran, Henige Thomas M. Method and apparatus for efficient modulo multiplication. Patent US №8Y17756B2, (2013).

[16] S. Tynymbayev, R. Berdibayev, T. Omar, S. Gnatyuk, T. Namazbayev, S. Adilbekkyzy. Devices for multiplying modulo numbers with analysis of the lower bits of the multiplier, Bulletin of National Academy of Sciences of the Republic of Kazakhstan, № 4, 2019, С. 38-45.

[17] Iavich M., Iashvili G., Gnatyuk S., Tolbatov A., Mirtskhulava L. Efficient and Secure Digital Signature Scheme for Post Quantum Epoch, Communications in Computer and Information Science, Vol. 1486, pp. 185-193, 2021.

MATRIX MULTIPLIER BY MODULO FOR CRYPTOGRAPHIC TRANSFORMATIONS

The main function of cryptographic methods and means of information protection is to ensure the confidentiality and integrity of data. Data encryption is carried out by specialized means (encryptors), which are based on a certain stable (secure) cryptographic algorithm (symmetric or asymmetric). There are three types of encryptors, that are most widely used for data encryption: hardware, software-hardware and software. Their main difference is not only in the method of encryption and the degree of reliability of data protection, but also it is the price, which often becomes a determining factor for users. Despite the fact that the price of hardware encoders is significantly higher than software, the difference in price is not comparable to a significant improvement in the quality of information protection. Hardware encryption has a number of significant advantages over software encryption, one of which is higher performance. Hardware implementation guarantees the integrity of the encryption process. In this case, the generation and storage of keys, as well as encryption is

carried out in the encryption board itself, and not in the computer's RAM. Given this, the development of high-speed operating units of hardware processors for asymmetric encryption, despite their high cost, is an urgent scientific and applied task. This study considers up-to-date approaches to multiplication of numbers by modulo. The algorithm of multiplication with stepwise formation of partial and intermediate residues is investigated, which in turn does not require preliminary calculations, and all calculations do not go beyond the range of the bit grid of the module. As a result, a synchronous matrix multiplier was developed, which contains n blocks of schemes I, n-1 FPR and a single FIR with an intermediate residue register. These results will be useful for cryptographic transformation in the systems with high speed and security requirements, for example in critical information infrastructure of the state.

Key words: public key cryptosystem, hardware encryption, remainder generator, multiplier.

Луцький Максим Георгійович, доктор технічних наук, професор, ректор Національного авіаційного університету.

Maksym Lutskyi, doctor of technical sciences, professor, rector of the National Aviation University.
E-mail: maksym.lutskyi@nau.edu.ua
Orcid ID: 0000-0003-1678-3196

Тинимбаєв Сахибай Тинимбайович, к.т.н., професор кафедри інформаційних систем та кібербезпеки Алматинського університету енергетики та зв'язку.

Sakhybay Tynymbayev, PhD, Professor of Information Systems and Cybersecurity Academic Department, Almaty University of Power Engineering and Telecommunication.
E-mail: s.tynym@gmail.com.
Orcid ID: 0000-0002-9326-9476.

Гнатюк Сергій Олександрович, д.т.н., доцент, заступник декана Факультету кібербезпеки, комп'ютерної та програмної інженерії Національного авіаційного університету.
Sergiy Gnatyuk, DSc, Associate Professor, Vice-Dean of the Faculty of Cybersecurity, Computer and Software Engineering, National Aviation University.
E-mail: s.gnatyuk@nau.edu.ua.
Orcid ID:0000-0003-4992-0564.

Бердибаєв Рат Шиндалійович, доцент кафедри інформаційних систем та кібербезпеки Алматинського університету енергетики та зв'язку.
Rat Berdibayev, PhD, Associate Professor of Information Systems and Cybersecurity Academic Department, Almaty University of Power Engineering and Telecommunication.
E-mail: r.berdybaev@aues.kz.
Orcid ID: 0000-0002-8341-9645.

Поліщук Юлія Ярославівна, аспірант PhD Національного авіаційного університету.
Yuliia Polishchuk, PhD student, National Aviation University.
E-mail: liya7954@gmail.com.
Orcid ID: 0000-0002-0686-2328.